ROUTING AND RECORD SHEET

SUBJECT: (Optional)

FROM:
Daniel A. Childs, Jr.
Comptroller

EXTENSION: [redacted]

NO. COMPT 86-1741

STAT

DATE

TO: (Officer designation, room number, and building)	DATE		OFFICER'S INITIALS	COMMENTS (Number each comment to show from whom to whom. Draw a line across column after each comment.)
	RECEIVED	FORWARDED		
1. OCA				
2.				
3.				
4.				
5.				
6.				
7.				
8.				
9.				
10.				
11.				
12.				
13.				
14.				
15.				

[redacted]

Central Intelligence Agency

Washington, D.C. 20505

COMPT 86-1741

Also sent to:

[redacted] 25X1

C/IHC
IC Staff

1 DEC 1986

[redacted] 25X1

Director, Program and Budget Staff
Intelligence Community Staff
Washington, D.C. 20505

Dear ~~Bill:~~ Bill:

Enclosed is CIA's report on computer auditing capabilities and labelling standards, as requested in the DCI's 1988-1992 National Foreign Intelligence Guidance.

[redacted] 25X1

Daniel A. Childs, Jr.
Comptroller

Enclosure:
As stated

cc: [redacted] 25X1

Admin-Internal Use Only
When Separated From
Secret Attachment

[redacted] 25X1

~~SECRET~~

CENTRAL INTELLIGENCE AGENCY

COMPUTER SECURITY REPORT

NOVEMBER 1986

INTRODUCTION

This report responds to the DCI's 1988-1992 National Foreign Intelligence Guidance which requires a status report on the computer security efforts from the Intelligence Community agencies. All of the technology described in this report is being developed to run on large IBM or IBM-compatible computers. The technology will be made available on request to users in the Intelligence Community.

AUDITING COMPUTER SYSTEMS

This Agency pursues a very aggressive computer security audit program. Begun by the Office of Security in 1982 with one individual assigned part-time to the effort, the program has since grown to three man-years dedicated to the auditing of all 12 of the Agency's major main frame Automated Information Systems (AIS), including VM, CAMS and 4C. The program has proven very successful in several respects. A number of computer abuse cases have been detected resulting in the revocation of clearances, employee terminations, and one individual being reported to the Justice Department for possible criminal prosecution. In addition, the audit program has helped to identify a number of security weaknesses in the operating systems of the Agency's main frame computer, and appropriate steps were taken to correct them.

The present auditing program includes the use of various commercial database software (i.e. Creatabase by NDX and ACF 2) to process audit trail information produced on our main frame computers. Essentially, three significant system parameters are required: 1) accountability through unique individual user passwords; 2) 2.2 billion bits of on-line storage for the storage and retrieval of accounting records captured in daily transactions; and, 3) site licenses to use the software for extracting the information. At present, the auditing program is still primitive and relies mainly on a manual and limited automated review of day-old data. Failed attempts to "log-on" to a system and failed attempts to connect to a "mini-disk" are reviewed on a daily basis. All other user activity is recorded and stored for future reference.

Two steps are needed to improve the audit program. First, a mechanism is required to search the audit trail information to identify potential incidents of abnormal user activity not flagged as an actual violation. Second, automated tools are needed to quickly search and process this information. In FY 1987 we will contract with a firm experienced in searching large databases and developing software to correlate seemingly unrelated events to develop these capabilities.

This contractor will develop a user profile system that will ensure that any action not conforming to the user's standard profile will be flagged and reported to an auditor. For example, a user might normally log on the VM system between 0900 and 1100 at a workstation located in an outbuilding and only link to mini-disk A, B, and C. If that user or someone using his/her userid and password logged on to VM from another building, at a different time, or to another mini-disk, a flag would go up. An auditor would then determine if the user were legitimate. This new auditing capability will be available within six months after the contract is signed and will operate on all Agency main frame systems. The maintenance costs for the new program have not yet been determined.

Work is also currently ongoing to develop Artificial Intelligence (AI) as a tool in the security auditing process. Our goal is to use AI to provide system memory identifying potential paths of abnormal user activity and to provide flags to the auditor. Usable results are expected in about two years.

AUTOMATED LABELING

The labeling (classifying) of information is a basic security requirement that is a mandatory national policy regardless of the form used to store the information (paper, electronic, etc.). The access to information is regulated by matching an individual's access rights and clearances to the document's sensitivity labels. The primary difference between labeled paper and labeled electronic data is the system and procedures that allow access to the information.

In the paper world, the control of access to information is controlled by human checks and balances. With electronic data stored and transferred in automated information systems or contained on magnetic media, the traditional human checks and determinations are, in most cases, no longer applicable. It is up to the computer to make the required access determinations.

Automated labeling will provide a computer the capability to enforce the "need-to-know" principle regarding user access to data. Labeling is a key element that will enforce a deliberate management decision as to what mandatory, discretionary, and flow controls are required for sensitive data stored in ADP equipment. The computer will enforce this process by comparing a user's previously defined clearances and accesses with the label of the data in question and then make a determination as to whether or not access should be granted.

To date, there is no labeling "standard" used by the Community. Some time in the future there may be a requirement to network this Agency's computer systems with computers belonging to various members of the Community. Standard labeling will be required to ensure the security of the data on the system.

In FY 1986, we contracted for the first phase of a data labeling initiative. This contract will develop a machine readable internal data label standard for use within CIA. The statement of work, however, anticipates expanded use of the label standard to include compartments and other restrictive caveats used within the Intelligence Community. If successful, this label model will be adapted as the standard for use within the community.

This initial contract will provide (1) an internal label representation with the functional design specifications required to manage the label, and (2) a label representation for use on transportable magnetic media (i.e., tapes). A follow-on effort is planned to implement the internal label model on one of the Agency's Critical Systems. The 4C system would probably provide the most suitable test environment because of the type of data it contains.

Too may unanswered questions remain to determine the resource impact of this effort at this time. For example, will we need to label all existing data? If so, can this process be automated? How will the addition of the label affect the operation of the various systems? Will the label be compatible to all systems and can it be transported from one system to another?

SUMMARY

Funds are allocated in the FY 1987 COMPUSEC initiative specifically for auditing and labeling. The primary goal will be to improve upon the existing auditing capability and to develop a data labeling standard for the Agency's network. The security focus for the outyears, FY 1988 and FY 1989, will be to concentrate on improving the security and control of information processed and stored on personal computers, which is the number one priority for the Intelligence Community. Once these capabilities exist, they will be made available for community members